Kiss from a Rogue: Evaluating Detectability of Pay-at-the-Pump Card Skimmers

Nolen Scaife, Jasmine Bowers, Christian Peeters, Grant Hernandez, Imani N. Sherman,
Patrick Traynor, Lisa Anthony
University of Florida
{scaife, jdbowers, cpeeters, grant.hernandez, shermani}@ufl.edu, {traynor, lanthony}@cise.ufl.edu

***Abstract*—Credit and debit cards enable financial transactions at unattended "pay-at-the-pump" gas station terminals across North America. Attackers discreetly open these pumps and install skimmers, which copy sensitive card data. While EMV ("chip-and-PIN") has made substantial inroads in traditional retailers, such systems have virtually no deployment at pay-at-the-pump terminals due to dramatically higher costs and logistical/regulatory constraints, leaving consumers vulnerable in these contexts. In an effort to improve security, station owners have deployed security indicators such as low-cost tamper-evident seals, and technologists have developed skimmer detection apps for mobile phones. Not only do these solutions put the onus on consumers to notice and react to security concerns at the pump, but the efficacy of these solutions has not been measured. In this paper, we evaluate the indicators available to consumers to detect skimmers. We perform a comprehensive teardown of all known skimmer detection apps for iOS and Android devices, and then conduct a forensic analysis of real-world gas pump skimmer hardware recovered by multiple law enforcement agencies. Finally, we analyze anti-skimmer mechanisms deployed by pump owners/operators, and augment this investigation with an analysis of skimmer reports and accompanying security measures collected by the Florida Department of Agriculture and Consumer Services over four years, making this the most comprehensive long-term study of such devices. Our results show that common gas pump security indicators are not only ineffective at empowering consumers to detect tampering, but may be providing a false sense of security. Accordingly, stronger, reliable, inexpensive measures must be developed to protect consumers and merchants from fraud.**

I. Introduction

Credit and debit cards are critical to the modern financial ecosystem. Consumers and merchants rely on the security and convenience of these cards for fast transactions without the need to handle cash. In North American gas stations, the nearly-ubiquitous deployment of pay-at-the-pump has eliminated the need for additional employees and allows consumers to more quickly obtain fuel. This technology is used by nearly three-quarters of Americans each day who purchase gasoline [39].

The popularity of these unattended payment terminals has made them an attractive target for attackers seeking to obtain sensitive payment card data. The primary means for these attacks are internal skimmers [45], which are physical devices that perform a man-in-the-middle attack inside the gas pump. The deployment of EMV ("chip-and-PIN") terminals would appear to be a straightforward fix to this problem. However, deploying EMV can cost upwards of $15,000 USD per pump and, due to federal safety standards, must be inspected by a licensed technician (who are historically in short supply) [21]. Accordingly, between the expense of replacement and the business lost due to downtime before re-certification, the overwhelming majority of gas stations have elected to continue to use magnetic stripe technology. In lieu of EMV, the industry has instead widely deployed tamper-evident seals and other indicators to alert consumers and employees to potential skimming attacks. The use of these indicators represents a shift in responsibility for detecting tampering from the operator to the consumer. Specifically, the use of such mechanisms assumes that consumers are able to identify and interpret security indicators and that they can or will take appropriate action.

In this paper, we seek to comprehensively evaluate a single research question: *do mechanisms created to alert consumers of gas pump point-of-sale skimmers provide reliable protection?* To answer this question, we evaluate the software, hardware, and physical security mechanisms used to attempt to achieve these ends. In so doing, we make the following contributions:

- **Analysis of Bluetooth Skimmer Detection Apps:** Recent best practices suggest that consumers can better protect themselves against pump skimmers through Bluetooth skimmer detection apps. We perform a comprehensive software teardown of all known Bluetooth skimmer detection apps in the App Store (iOS) and Google Play (Android) markets. We identify the skimmer characteristics that each app uses for detection.
- **Forensic Hardware Analysis and Detection Countermeasures:** Through our partnerships with three law enforcement agencies, we were able to examine six internal skimmers confiscated as part of separate criminal investigations. We first perform a comprehensive forensic analysis and characterization of each device. We then test the effectiveness of each app, and show that few are able to reliably detect *any* skimmer. Moreover, we demonstrate that simple evasions make it possible for skimmers to evade detection by *all* apps.
- **Long-Term Study of Recovered Skimmers:** Using data collected between 2015 and 2018 by the Florida Department of Agriculture and Consumer Services, we perform the first long-term study of gas pump skimmers. We begin by discussing the challenges of deploying tamper-evident seals in this setting; the reports in this dataset demonstrate that this legally mandated defensive mechanism is overwhelmingly ineffective at deterring skimming attacks. Specifically, we observe that more than 90% of annotated

reports in which gas pump skimmers are found have approved security measures in place.

The remainder of this paper is organized as follows: Section II provides background on the problem of gas pump skimmers; Section III details the mechanisms of skimmer detection apps; Section IV provides a breakdown of internal skimmers and evaluates the detection apps' ability to detect skimmer characteristics; Section V discusses the challenges of deploying tamper-evident seals, and how they have largely failed in practice; Section VI offers possible solutions and future work; Section VII discusses related work; and Section VIII gives concluding remarks.

II. Background

Magnetic stripe card data is stored as unprotected plaintext. Any reader that comes in contact with the card can obtain a complete copy of the data, and this data can be rewritten to a different card. Accordingly, attackers use card reading devices (also known as *skimmers*) to acquire the sensitive account data from victims' cards.

Skimmers are produced in a variety of form factors and can be applied in many ways to a target device [45]. We evaluate the problem of gas pump skimming attacks, which are believed to be predominantly internal today—attackers physically open the target pump, and insert the skimmer between the card reader module and the mainboard. This device performs a classic man-in-the-middle attack on the reader's serial connection, allowing the skimmer to read and store card data while providing the pump the same data. From the victim's perspective, there is no visible change to the payment flow. Figure 1 shows two skimmers we obtained from law enforcement; we examine these and others in Section IV.

Installing these skimmers requires attackers to open an access door to the terminal equipment and install the skimmer without drawing suspicion from employees or other customers. To secure pumps against these attacks, Florida statutes require pump operators to deploy at least one of these security measures: a tamper-evident seal, a device that disables the pump or payment terminal when opened, a card reader that encrypts card data before transmission, and/or another approved control.[1] Gas pump payment fraud results in millions of dollars in losses per year in total despite costing stores an average of $700 per year [37]. This asymmetry causes individual stores to have low motivation to solve this problem. The high cost of retrofitting newer payments technologies such as EMV [38], high security locks, alarms, and other controls makes deploying these solutions financially unsound.[2]

To reduce the risk for attackers, some skimming devices have a wireless data retrieval mechanism (e.g., Bluetooth) to avoid the need to reopen the pump and to reduce the risk of detection. The introduction of Bluetooth-enabled skimmers fostered an arms race, which has led to the production of smartphone apps for detecting skimmers. We analyze these apps and their detection mechanisms in detail in Section III. We evaluate these apps against skimmers confiscated by law enforcement in Section IV. We examine the pervasiveness, utility, and effectiveness of seals in Section V.

Finally, while consumers in the United States enjoy limited liability for credit card purchases, fraudulent charges onto debit or prepaid cards immediately remove funds (i.e., from a bank account) until the bank releases those funds. In cases such as debit cards, the consumer may only have a limited time to report fraud before being fully liable for the charge, and it may take months to regain control of contested funds (if ever). These costs are initially absorbed by banks and payment networks. This has motivated them to force the deployment of EMV (at the merchants' expense) to curb rising card fraud. Accordingly, card fraud results in real costs to consumers and merchants.

III. Skimmer Detection Apps

Increasingly desperate to protect themselves against skimmers, hundreds of thousands of consumers have downloaded skimmer detecting applications for their smart devices. Given that some gas pump skimmers rely on Bluetooth radios to reduce the risk to their owners of being caught while physically retrieving these devices, such an approach is intuitive and similar techniques have been used to detect rogue cellular base stations [19] and Wi-Fi access points [34], [17]. However, the efficacy of these apps, which represent the only electronic detection method available to consumers, has not previously been measured.

A. Methodology

Using skimming-related terms (e.g., skimmer, skimmer detection, skimming, skim, gas pump), we discovered five Android applications in the Google Play Market and two applications in the Apple App Store that purport to detect skimmers. For the Android applications, we downloaded and decompiled their Dalvik bytecode using the JEB decompiler [49]. We then examined the decompiled source of each app to determine the mechanism they use to detect skimmers. For iOS we used IDA Pro 7.0 [44] to view the ARM64 assembly, LLDB [42] for debugging and breakpointing, and Frida [43] for function interception. We used two test devices: a jailbroken iOS 10.3.2 device to decrypt the iOS IPA files using Clutch and a stock iOS 11.3.1 device for dynamic analysis. An overview of these results are shown in Table I. We also test these apps with real skimmers in Section IV; below, we discuss our analysis of the detection methods of each app.

B. Results

Skimmer Scanner (A). This app was developed based on a SparkFun article [3]. The application is a C# Xamarin app and is open-source. Rather than decompiling the app, we examined the source code from GitHub [4].

This app is the most conservative in its detection mechanism; a series of five steps must successfully complete to produce a red alert, the app's most severe alert. Each of these steps is specific to the specific skimmer model discussed in the SparkFun article. The app first scans for Bluetooth devices,

[1] To the best of our knowledge, the list of alternative approved controls, if any, is not published.

[2] For readers convinced that EMV is a drop-in solution to this problem, please read [21] for industry perspective. One of the greatest challenges in security is actual deployment, and solutions that ignore real world constraints and incentives are rarely deployed successfully.

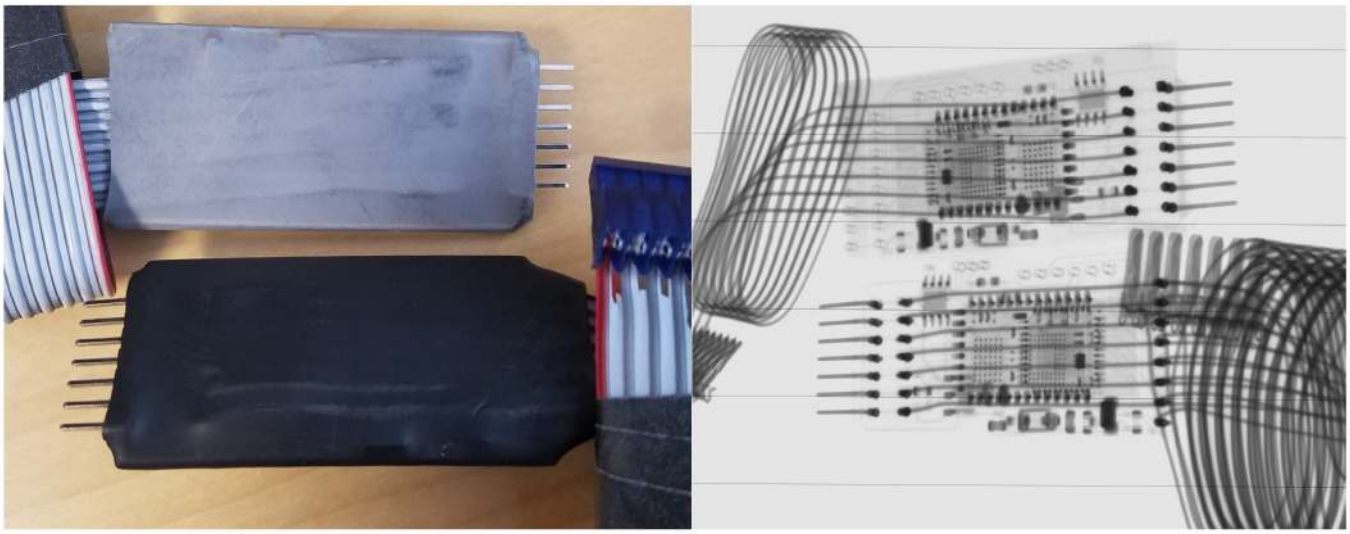

Fig. 1: Two internal skimmers confiscated from gas pumps by law enforcement. On the left, the skimmers are shown as they appear when discovered. On the right, an X-ray image taken with a Bruker SKYSCAN 2211 Nano-CT System. We photographed these skimmers before removing the outer heat-shrink to ensure we did not damage them during examination.

ID	Name	Version	Platform	Downloads	Detection Mechanism
A	Skimmer Scanner	1.4	Android	100,000+	Name==HC-05, PIN==1234, Query/Response
B	ATM Skimmer Detector	1.0	Android	10,000+	Name==HC-05 || Name==HC-06, PIN==1234, Query/Response
C	Skim Plus	4.1	Android	1,000+	MAC address matches
D	Skimmer Protection Scanner	4.1.3	Android	Removed	None
E	Dark Skimmer Protector	4.1.3	Android	Removed	None
F	Skimmer Map	1.0	iOS	Unknown	Crowd-sourcing
G	Card Skimmer Locator	1.0	iOS	Unknown	Name.Length $>$ 14

TABLE I: We analyzed all five apps (A–E) on the Google Play Market and both apps (F–G) on the Apple App Store which claim to detect skimmers. Each app's detection mechanism is listed; all listed items must match for detection to occur.

then performs the steps as each in-range Bluetooth device is discovered. These are:

1) Check if the Bluetooth device's name is `HC-05`. If this check passes and any subsequent check fails, the app warns that a suspicious device is present.
2) The app attempts to pair with the device using PIN `1234`.
3) The app creates a Bluetooth serial socket to the device.
4) The app sends a single byte, `0x50`, to the device.
5) The app checks the returned data; if the data begins with byte `0x4D`, the app warns that a skimmer may be present.

ATM Skimmer Detector (B). This app's description identifies it as being capable of detecting both ATM and gas pump skimmers (and specifically identifies the `HC-05` skimmer).

This app's functionality is similar to Skimmer Scanner (A). In Step 1, however, the device's name can be either `HC-05` or `HC-06` (case insensitive). The remaining steps are identical.

Skim Plus (C). Like Skimmer Scanner (A), this app is a C# Xamarin app except the source code is not publicly available. Xamarin apps package the compiled application with portions of the Mono framework inside an Android app. After unpacking the Android APK, we extracted the compiled DLL and decompiled it with JetBrains dotPeek.

Skim Plus detects apps solely on MAC address matching. For each discovered Bluetooth device, the app checks to see if its MAC address begins with:

- `00:0B:CE` (assigned to Free2move AB)
- `EC:E9:F8` (assigned to Guang Zhou TRI-SUN Electronics Technology Co., Ltd)
- `00:06:66` (assigned to Roving Networks)
- `20:16` (multiple assignees)
- `20:17` (unassigned)

We checked each MAC prefix with the IEEE Standards Registration Authority [5] and noted its assignee. The `20:16:00`–`20:16:FF` block has multiple assignees, including Intel (`20:16:B9`) and Liteon Technology Corporation (`20:16:D8`). At the time of writing, the `20:17:00`–`20:17:FF` block has no assignees. Aside from the fragility of this approach, the appearance of these two-byte MAC prefixes greatly increases the risk of false positives. Furthermore, since `20:17` is not assigned, the manufacturers of any devices using this prefix are arbitrarily selecting MAC addresses. We discuss this in greater detail in Section IV.

The app does not attempt to connect to any device, instead alerting if it discovers any matching Bluetooth device. The "Possible Skimmers Found!" alert is displayed with an icon indicating the matching device's signal strength. The app is capable of sending the location of the skimmer to `ronzoo.com` via HTTP (this is presumably how the app produces mapping data for other users). Furthermore, this API does not appear to have any authentication capabilities; as a result, an attacker could flood the server with false reports of skimmers.

Skimmer Protection Scanner/Dark Skimmer Protector (D/E). Finally, these two apps are Apache Cordova apps which display a rendered HTML/JavaScript view to the user. We examined both the decompiled bytecode and the HTML/JavaScript elements unpacked from the APK. There are no functional differences between these two apps; the icon, logo, splash screen, background color, and advertising ID are the only code differences.

These apps do not detect skimmers. Once the user activates the scan, the apps display an ad and a progress bar, sleep for five seconds, and display a list of the phone's bonded Bluetooth devices. Once this process completes, the user is shown the message "NO SKimmer found this scan not found any device use skimmer hardward plz be bhide some device skimmer !!" [sic] and a chart with random values is displayed.

Soon after our analysis, these two apps were both removed from the Google Play store. We captured the apps' full descriptions before they were removed; both apps are non-obviously described as a simulation of skimmer detection. The apps do not appear to be simulations once installed or running; accordingly, we believe few users would realize that these apps perform no checks.

Skimmer Map (F) To understand the application's behavior, we first ran it on our iOS 10 device. The application displays a map and current location, and it appears as though it should overlay locations of reported gas pump skimmers. During testing, however, we confirmed that the map was not being populated with any results. It does not appear to contain any functionality for detecting skimmers on its own (e.g., via Bluetooth).

We decrypted the IPA file using a jailbroken device, which allowed us to perform static analysis on the application binary using IDA Pro. We discovered a single URL in the string references: `http://skimmermap.gaspumpsentry.com/`. At the time of analysis, this domain name did not resolve to a valid IP using DNS. Although `www.gaspumpsentry.com` still resolves to a related site, we suspect that this app is abandoned by the developer. Without access to the crowdsourced skimmer data, this application is effectively broken.

Card Skimmer Locator (G) This application claims to scan for skimmers that use Bluetooth Low Energy (BLE). It either displays a list of suspicious device names or a checkmark and "None Found". In practice, the application immediately displays "None Found" even in the presence of an HC-05 skimmer. To better understand this behavior, we decrypted it and performed static analysis using IDA Pro. We found proper code to listen for discovered BLE devices, but during our dynamic analysis using Frida and LLDB, we observed that the app would immediately display "None Found" if a device was detected with a `NULL` device name. We examined the application code but could not find any hardcoded suspicious device names like we discovered with other apps. More reverse engineering yielded that the app displays any detected BLE device with a name greater than 14 characters as "suspicious."

None of the skimmers we have examined use BLE, limiting the effectiveness of this application. The skimmers in our possession use Bluetooth Classic, for which iOS does not provide public scanning APIs. Therefore, it is not possible to publish an application to the App Store that scans for Bluetooth Classic skimmers on iOS [10], limiting the use of this platform for skimmer detection.

C. Lessons Learned

In theory, tools designed to help consumers detect gas pump skimmers are ideal solutions. However, from our teardown of these skimmer detection apps, we see that their ability to detect skimmers is limited. Some of the apps we examined do not actually detect skimmers at all, but advertise themselves as such. These apps provide users with a false sense of security and make it a challenge for users to identify which apps actually work at all. The only non-abandoned skimmer detection app for iOS does not function properly, limiting even the possibility of detecting skimmers via smartphones to Android users. The apps that are not clearly broken are all similar in their detection methods and rely on specific characteristics as well as historical data of skimmers to identify them. Although these apps are limited, their current use is evidence that the assistance of effective skimmer detection technology is needed.

Furthermore, we are concerned by the apps that establish connections to candidate devices. These connections may run afoul of laws that prohibit access to others' electronic devices (e.g., the Computer Fraud and Abuse Act - 18 USC § 1030). Since the Bluetooth serial adapters these apps are designed to detect can be used in legitimate, non-skimming devices, the issuance of a command to these devices may have ill effects.

IV. Hardware Analysis

We partnered with four law enforcement agencies (the Florida Department of Agriculture and Consumer Services, the Gainesville Police Department, the Alachua County Sheriff's Office, and the NYPD Financial Crimes Task Force) and received six internal gas pump skimmers that had been released from evidence. In this section, we characterize the skimmers and evaluate whether smartphone apps appropriately leverage these characteristics for detection. After analyzing the initial state of the skimmers, we test with the apps, discuss evasion techniques, and demonstrate evasion is possible.

A. Hardware Teardown

Table II lists each skimmer and its hardware composition. We assign an identification number to each skimmer and discuss the general operation of the devices as well as specific aspects of each skimmer.

Each skimmer has similar hardware components and functionality. Figure 2 shows the major common hardware components. The skimmer is inserted between the magnetic stripe card reader and the pump's mainboard, allowing it to intercept the card data. To do this, the existing card reader is disconnected and a flat ribbon cable on the skimmer is connected to the reader. The skimmer is then connected to the mainboard using another set of pins, re-establishing the connection through the skimmer. The microcontroller on the skimmers then processes the data as it is received and stores it in flash memory. Each skimmer is equipped with a data retrieval feature (e.g., a Bluetooth module is shown in Figure 2) that allows a criminal to obtain the data on the flash memory at a later occasion.

Skimmer ID	Connection Cables	Microcontroller	Flash Memory	Communication Method	Radio Module	BT Name	BT PIN	BT MAC Address
S-01	Card Reader	PIC 18F4550	ST 25P16VP	Bluetooth	HC-05	HC-05	1234	20:17:01:09:24:37
S-02	Card Reader and PIN Pad	PIC 18F4550	ST 25P16VP	Bluetooth	HC-05	HC-05	1234	20:16:11:21:06:07
S-03	Card Reader and PIN Pad	PIC 18F4550	MXIC 25V8006EM	Bluetooth	RN42	RNBT	1234	00:06:66:81:E9:FB
S-04	Card Reader	AT Mega 8515	PCT 25VF040B	USB	N/A	N/A	N/A	N/A
S-05	Card Reader and PIN Pad	PIC 18F4550	MXIC 25V8006EM	Bluetooth	RN42	RNBT	1234	00:06:66:E7:CA:C1
S-06	Card Reader	PIC 18F4550	ST 25P16VP	GSM	SIM800	N/A	N/A	N/A

TABLE II: The breakdown of each skimmer's hardware components, connects to gas pumps, and their method of transmitting data. Each skimmer is assigned an ID number for reference. The table also provides some of the settings on each skimmer's communication module when we received them.

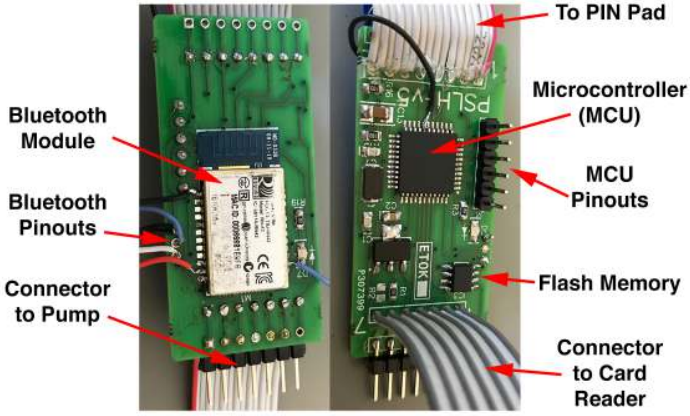

Fig. 2: The front and back of Skimmer S-03 with the major hardware components identified. We added the non-ribbon wires during analysis.

Consumers using debit or credit cards often need to enter a PIN or ZIP code to successfully authorize their cards. Since this data is also valuable to attackers (e.g., for cloning debit cards and cashing out at ATMs), many skimmers also include a passthrough mechanism for capturing PIN pad entry. We examine the specific components of each skimmer and summarize their construction below:

Skimmer **S-01** is built using a PIC-based microcontroller and an STMicroelectronics flash memory chip for storing card data. The skimmer uses an HC-05 Bluetooth module for wireless data retrieval. When we took possession of this skimmer, it was configured with the name `HC-05` and PIN `1234`.

Skimmer **S-02** is identical to Skimmer S-01, except that it is also capable of intercepting PIN entry directly from the PIN pad via an additional passthrough cable.

Skimmer **S-03** is similar in construction to Skimmers S-01 and S-02. However, the flash memory chip is different on this skimmer and it uses an RN42 Bluetooth module. Like S-02, this skimmer is also capable of intercepting PIN entry.

Skimmer **S-04** differs most significantly from the others we examined. This skimmer transfers card data via a wired connection and does not use a Bluetooth or other wireless communication module. Both the processor architecture and flash memory differ, making this skimmer the most unique of the ones we received. This skimmer is not capable of capturing PIN pad data (like S-01).

Skimmer **S-05** is identical to Skimmer S-03. The voltage regulator on this module had burned out and damaged the cable that attaches the card reader. Due to this, we needed to apply voltage directly to the microcontroller to power the device on. This skimmer is also able to capture PIN pad data.

Skimmer **S-06** is similar is design to Skimmers S-01, S-02, S-03, and S-05, but is equipped with a cellular communication module as opposed to Bluetooth. The cellular module is a SIMCom SIM800 GSM module that transmits voice and SMS over the GSM network. The processor and flash memory chips are identical to those in Skimmers S-01 and S-02. This skimmer only has a cable for intercepting card readers; the PCB has unused pads that can accommodate a cable to intercept PIN pad data.

Of the six skimmers we received, four use Bluetooth (two with HC-05 modules and two with RN42 modules) as their data retrieval mechanism and one uses cellular communication over the GSM network. The sixth uses a USB connector which requires a criminal to physically retrieve the skimmer in order to obtain card data. Accordingly. Bluetooth based detection apps can not find all of the devices currently being used to skim gas pumps.

B. Bluetooth Modules

As discussed in Section III, smartphone skimmer detection apps indicate the presence of skimmers based on characteristics of their Bluetooth communications. We discovered in that section that apps use four main criteria to determine if a Bluetooth module belongs to a skimmer: the name the module broadcasts, the password to connect to the module, the operation of the device once connected to the Bluetooth module, and the module's MAC address.

Both the HC-05 module and the RN42 module accept AT-style reconfiguration commands via serial communication. The manufacturers of both modules provide documentation that lists the valid command set, however many commands are unavailable wirelessly; the devices must have a physical configuration pin set in order to accept most critical commands (e.g., name and PIN configuration).

All four Bluetooth-enabled skimmers in our possession provide direct pinouts to the serial pins on the Bluetooth modules as is shown in Figure 2. Using these pins we were able to dump the initial configuration and alter existing settings on the modules. All four modules were still in their default settings, including the name and PIN. Table III provides a list of AT commands we used to view and alter the settings.

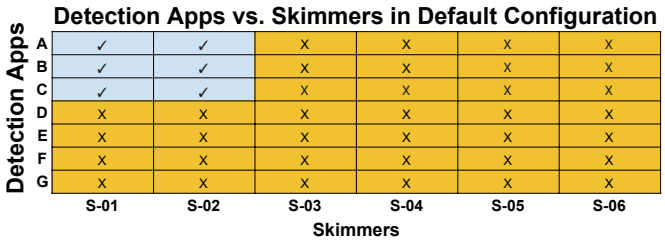

Fig. 3: We powered on each skimmer and attempted to detect them using each app. The blue squares indicate a detection, while the orange squares indicate that the app could not detect the skimmer. Because S-03 and S-05 were not set up correctly when we received them, they were not detected. As expected, no applications detect S-04 since it does not have a Bluetooth module.

Purpose of Command	HC-05	RN42
Get Module Password	AT+PSWD?	GP
Get Module Name	AT+NAME?	t
Get Module MAC Address	AT+RNAME?	GB
Set Module Password	AT+PSWD=<password>	SP,<password>
Set Module Name	AT+NAME=<name>	SN,<name>

TABLE III: A list of AT commands for changing parameters on the Bluetooth modules in efforts to prevent detection. The AT commands for the HC-05 are in traditional format while they are simplified for the RN42. Many other commands exist for both modules and can easily be found in their documentation.

C. Detection Effectiveness

We powered on each skimmer without modification in our lab and attempted to detect them using the apps from Section III. The results of this experiment are shown in Figure 3. Apps A, B, and C successfully detected S-01 and S-02. Since Skimmers S-04 and S-06 do not have Bluetooth modules, they cannot be detected by any app. Apps D, E, and F are incapable of detecting Bluetooth skimmers; similarly, App G is unable to detect any of these skimmers as it only detects Bluetooth Low Energy (BLE) devices.

Skimmers S-03 and S-05 are equipped with an RN42 Bluetooth module and were not detected in their default configuration, though App C looks for this module's MAC address prefix. Upon further investigation, we discovered that this is because the RN42 does not transmit data without first being properly configured. Unlike the HC-05 module, the RN42 cannot simply be soldered into a circuit and begin transmission; these devices were in an initial configuration state and were not enabled. It is possible that these devices were deployed without the intent of being able to retrieve card data wirelessly, though we are unable to verify this. Skimmers S-03 and S-05 would be detected by App C if they were properly configured, however, they were not and we recorded them as undetectable. Even in the event that the modules were properly configured, the RN42 Bluetooth module possesses additional features that can prevent the device from being seen unless in the presence of a separate Bluetooth device that is currently broadcasting a predetermined MAC address.

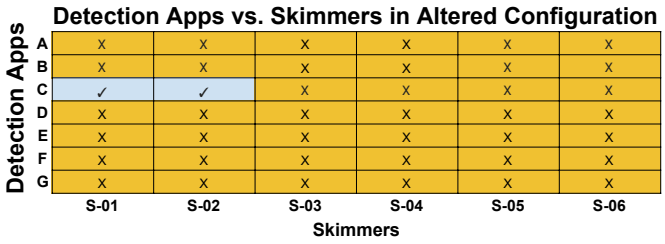

Fig. 4: This matrix shows which apps successfully detected each skimmer after configuration changes intended to evade. Apps A and B no longer work at detecting the skimmers. App C still detects Skimmers S-01 and S-02, as it only uses MAC Address as a detection criteria.

D. Evading Detection

Firmware Modifications As we have discussed, the detection methods are extremely brittle. Alterations can be made to the Bluetooth module's configuration that take advantage of the detection criteria, allowing it to appear as a normal Bluetooth device. Using the AT commands built into the firmware on the Bluetooth modules, it is trivial to change both the name and PIN. We modified the settings on each of the Bluetooth-enabled skimmers and ran each app again. For Skimmers S-01 and S-02, we changed the names to `Not a Skimmer` and the passwords to `5678`. Since the remaining skimmers did not have Bluetooth or it was not enabled, we excluded them from this experiment.

Figure 4 displays the app results after reconfiguring the Bluetooth modules. As expected, Apps A and B failed completely as their first check is the device's name. No other app improved its success rate after these changes, demonstrating that these simple changes dramatically affect the detectability of the skimmers. App C continued to detect the skimmers (shown with Skimmer S-03 in Figure 5), as it detects solely on MAC address prefix.

As we see in App C, this leaves the MAC address as the only remaining detection criterion. Though not as easy as with a standard computer Bluetooth module, spoofing the MAC address on the Bluetooth modules used in the skimmers is relatively simple. Because of the affordability of the Bluetooth modules used in skimmers, the features built into the standard firmware are limited. Neither module provides an AT command that allow the MAC address to be spoofed, however the developers of both modules provide software that allow users to overwrite the firmware. Adding Bluetooth spoofing to the firmware of both of these modules is entirely possible and would allow a user to eliminate the only remaining criteria that existing apps use for detection" would be reasonable. Other similar Bluetooth modules provide additional features such as MAC address spoofing.

Hardware Modifications Evasion can also be accomplished by selecting a Bluetooth module from a manufacturer that uses a different MAC address prefix. From our lab's collection of extra electronics components, we found four similarly-priced Bluetooth modules (from different manufacturers), that did not trigger a detection by any of the apps. All four are readily available from online electronics distributors and could easily be fitted onto a gas pump skimmer.

Fig. 5: This is a screenshot of a Google Pixel 2 running App C while Skimmer S-02 is powered on. The skimmer is the device second from the bottom of the list. The app indicates that the device is a skimmer by assigning it a red icon instead of green. This app also listed 14 other devices in this running instance that are not shown in this image; the user must scroll through the list to find the detected device.

Ultimately, further additions to the MAC prefix blacklist of App C is unsustainable. This use of such a list increases the number of possible false positives disproportionately to the number of skimmers it will detect. Any device that legitimately uses a Bluetooth module manufactured by one of the companies on the list will cause the app to create a false positive. Many Bluetooth devices are naturally at gas stations (including cars, phones, watches, etc.) that could potentially cause the application to induce an alarm.

Gas pump skimmers can also use wired communication methods that render the detection apps useless. Skimmer S-04 uses wired USB communication to transfer card data and cannot be detected by a smartphone. All of the skimmers can be dumped using a flash memory reader connected directly to the flash chip, provided the attackers are willing to risk retrieving the skimmer from the pump. Skimming attacks that use overlay skimmers need to be retrieved for recharging and data retrieval [45], so this is not a new method for obtaining card data.

Skimmers are also constructed using other wireless communication methods, such as Skimmer S-06 which uses SMS over GSM. Using a cellular module not only prevents detection by apps, but also allows the adversary to retrieve card data from nearly anywhere. Unlike Bluetooth, cellular communication is not able to be detected with a mobile device and creates legal concerns when it comes to intercepting data. Skimmer S-06 uses a fairly common and inexpensive cellular module that uses GSM networks. Though GSM technology is being phased out in the United States, GSM is still used in a variety of locations and is especially popular in many rural areas. Even if GSM were to be completely phased out, transitioning to a module that communicates over 3G networks is trivial and maintains the same detection challenges.

E. Lessons Learned

Out of the skimmers we received, two of the six did not use Bluetooth. Detecting these skimmers with a smartphone is not possible, regardless of app construction. The skimmer detection apps that exist are built on the assumption that all skimmers use similar Bluetooth modules for data retrieval, which is not the case. Though the idea of allowing anyone with a smartphone to detect nearby skimmers is seemingly attractive in terms of deployment, apps are not a solution to the problem of gas pump skimmers, and as these attacks evolve, they can only become less effective.

Considering Bluetooth skimmers alone, even the best skimmer detection apps are still not very effective, especially against a slightly determined attacker. From our hardware evaluation, only a few detection apps successfully detect skimmers, and most of these are easily evaded with trivial configuration changes. Though attempting to detect skimmers based on the MAC address of their Bluetooth modules will result in a successful detection regardless of configuration with standard firmware, this introduces substantially more false positives than true positives. Regardless, MAC address detection can be defeated in a variety of other ways.

V. Detecting Skimmers in Practice

As we have demonstrated through our software and hardware forensic analysis in the previous two sections, the tools available to consumers are ill-equipped to protect them from skimmers. Accordingly, we look to the mechanisms used by pump owners/operators to indicate that a compromise may have occurred. We then augment these observations using a long-term analysis of nearly four years of data collected by the Florida Department of Agriculture and Consumer Services on the location, condition, and security measures in place where gas pump skimmers have been found.

A. Tamper-Evident Seals

Tamper-evident seals [30] represent the only externally visible indicator of tampering (other than physical damage) of the security controls permitted by the State of Florida. Even if these seals are perfect, two problems arise: first, the seals would ideally be uniform in appearance and placement across locations. Figure 6 shows photos of pumps as we encountered them during the development of this work; these photos demonstrate real-world conditions. At a minimum, accurate inspection of seals requires consumers and employees to understand:

- **Presence:** Should a seal be present? Some stations apply seals and some do not, depending on other security features present (e.g., card readers that encrypt data prior to transmission as discussed in Section II).

(a) This pump is normal. It has a single, unbroken, correctly-placed seal.

(b) This pump has no seal.

(c) This pump has five seals.

(d) This pump has a single, unbroken seal. It is placed on the hinge of the door, however, making it unlikely to break if the door is opened.

Fig. 6: These photos demonstrate the real-world conditions in which tamper-evident seals must be evaluated. These seals are predominantly targeted at consumers, who must decide if a pump is safe to use before beginning a pay-at-the-pump transaction.

- **Placement:** Is the seal placed correctly on the pump? The seal needs to be placed where the seal will break or indicate (i.e., by showing "VOID") when the door is opened. Figure 6d shows a seal placed on the hinge of an access door. Such a placement is unlikely to indicate tampering if the door has been opened.
- **Intent:** What is the purpose of the seal? In some circumstances (such as shown in Figure 6c), the seals could be confused as an attempt to perform a short-term repair of a broken door or lock.
- **Identity:** Is this the *correct seal*? Figure 6 shows pumps that have branded seals (e.g., a Shell-branded seal at a Shell gas station) and Figure 7 shows a municipal seal. Replacement seals are readily available on the Internet, and the consumer or employee must know whether the seal visually matches the expected seal. Some seals include serial numbers, which can be logged and referenced later.
- **Indication:** Is the seal currently indicating tampering? Seals can be broken in a variety of ways, including stretching, displaying VOID (or similar), and slicing through the seal with a razor blade.

Second, these seals produce a *time of check to time of use* ("TOCTTOU") vulnerability which further requires consumer awareness and attention to detect tampering. This vulnerability stems from the time gap between when a skimmer is installed and when a person inspects the seal. The Federal Trade Commission recommends only daily checks by pump owners [53] but recommends consumers check seals before starting a transaction [52]. Advice to consumers from other organizations also suggests consumers should be looking for these security seals [41], [28]. Daily checks by owners can mitigate some damages, but an attacker could collect hundreds of cards' data at a high-traffic location in 24 hours. Accordingly, these indicators must target consumers, who have the best opportunity to immediately inspect the indicators before committing to a transaction. These seals often indicate to consumers that an employee should be notified of tampering as shown in Figure 8. Consequently, the deployment of low-cost tamper-evident seals has pushed the problem of keeping

Fig. 7: This style of seal is used throughout a municipality. In order to identify whether the correct seal is being used, consumers must be aware of the type of seal expected to be present.

Fig. 8: This is an image of a security seal on a gas pump we visited that instructs consumers to immediately notify an attendant that if the words "VOID OPEN" appear on it. The words "VOID OPEN" can be seen on this sticker, indicating tampering.

payments secure onto consumers.

B. Real-World Skimmer Data

We now measure the impact of these security measures by conducting a long-term study of skimmer incidents. In Florida, the Department of Agriculture and Consumer Services is responsible for the inspection of gas pumps, including the pay-at-the-pump payment terminals. This organization is legally capable of opening pumps for inspection and regularly inspects each of the pumps in Florida. They also collect reports from other law enforcement agencies when those agencies are informed of the presence of a skimmer (e.g., when an employee of a gas station identifies a skimmer).

We obtained records of all reported gas pump skimmers between 10 March 2015 and 14 November 2018 from the Florida Department of Agriculture and Consumer Services. The data in these reports provides insight into the locations and types of skimmers found and information about which

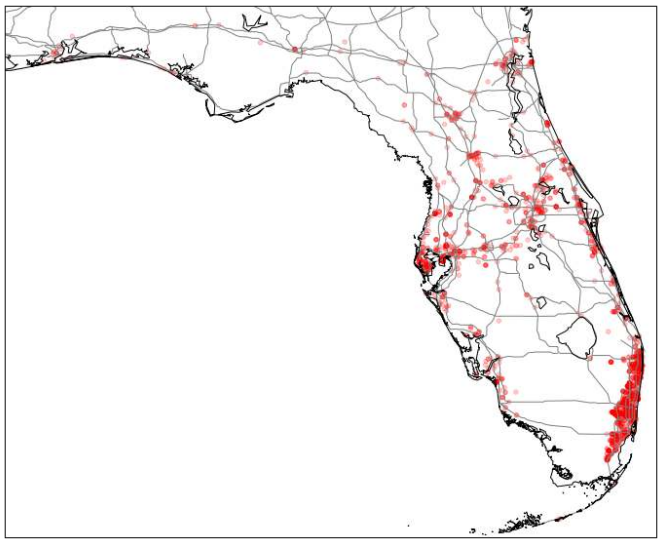

Fig. 9: A map showing all of the found skimmers in Florida from early 2015 until late 2018.

security measures were deployed on the pump at the time of detection. The reporting timeframe contains 1,588 reports covering 2,072 skimmers that were found across 953 unique locations. All of the skimmers found were internal skimmers. Below, we analyze this data and discuss the effectiveness of security mechanisms in place at the time of discovery.

1) Locations and Frequency: Using the raw data from the Florida Department of Agriculture and Consumer Services we resolved the contained addresses to latitude and longitude using the online geographical API, Geocodio.[3] We were able to successfully resolve 97% of the reports to global coordinates, with the remaining 3% failing to geocode due to coarse location or improper addressing. With the successfully translated addresses, we plotted the incidence of skimmers by location in Figure 9 using Cartopy and Matplotlib. Skimmer density correlates well to major population centers such as southeast Florida, but well-traveled interstates and state roads also appear to attract skimmers regardless of the surrounding area.

Anecdotal advice to avoid being skimmed may include a suggestion to avoid gas stations right off of an interstate, but evidence substantiating this intuition is difficult to come by. To examine this claim, we plotted the skimmers' distances to the nearest interstate exit in Figure 10. The data showed that nearly 50% of all skimmers were found within one mile of an interstate exit (state roads and highways not included). Further, 80% of all skimmers found were within three miles, and 90% within five. While this supports a claim that skimmers are less likely as distance from an interstate increases, we note there are conflating factors: First, some high-population areas are not immediately adjacent to an interstate. Second, increased density of skimmer activity near interstates may be related to higher density of gas stations near interstates. In general, this data suggests that driving more than five miles from an interstate would substantially reduce risk, but is unlikely to be convenient or viable for most consumers. It may be possible to obtain comprehensive data about gas station locations (our data includes only locations where skimmers have been found)

[3]https://geocod.io

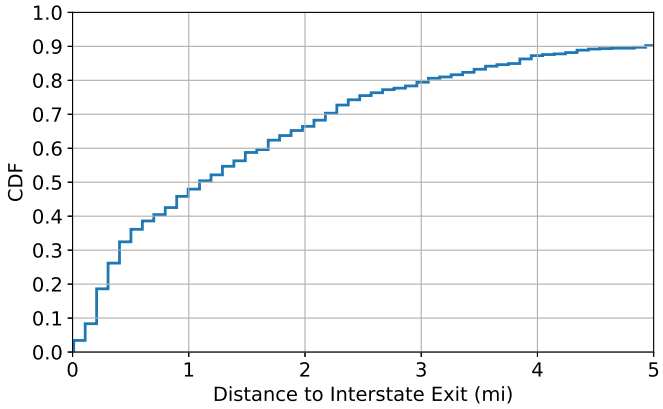

Fig. 10: A cumulative distribution showing the great circle distance in miles of all of the found skimmers in Florida to the nearest interstate exit.

and develop predictive models for skimming attacks, but we leave such a study to future work.

2) Security Measures: Two fields in each report specifically reference security measures used at a pump or station: "Security Measures in Place?" and "Comment." We were informed that the former notes whether or not the location where the skimmer was found was using any approved security measure [1]. 300 (18.9%) answers to "Security Measures in Place?" were blank and 42 records (2.6%) contain an answer other than "Yes" or "No" (this text was analyzed alongside the comments below). 1,127 (90.4%) of the remaining records indicate measures were in place and 119 (9.6%) indicate they were not.

To reiterate: the data in these reports describe events in which one or more skimmers were found to be present, and this data overwhelmingly shows existing security measures are ineffective at deterring skimmers.

Comments Analysis. The Comments field is a free-form field, so we consider the comments to be equivalent to a free response question asking for any additional information. To identify major themes [12], two researchers coded 1,190 reports that included information in this field. Such an analysis aids in understanding the state of the security measures of the pump at the time a skimmer was detected, as written by the reporter. One researcher open-coded the entire set and generated a set of codes or themes representing which security measures were specifically mentioned in the reports, their condition, and how they were discovered. The second researcher then coded the entire set using the codebook. We met to discuss if any errors were found in the codebook, and no emergent themes or errors were discovered. We calculated inter-rater reliability on the coded data using Cohen's kappa. Since a comment could have multiple codes assigned to it, we first converted each code into a binary yes/no variable to compute agreement on presence or absence of the code. The average Cohen's kappa over the 30 codes was κ=0.94 (min=0.73, SD=0.09), which corresponds to "almost perfect" agreement [32]. Most remaining disagreements were related to different interpretations of ambiguous grammar. For example, the two researchers disagreed on whether "Pumps have properly placed security tape/pump had fake seal and bent extra security lock" (524) meant that the pump had an extra (additional) security lock or an extra security (high security) lock. In cases of disagreement, those codes were discarded for our quantitative results.

We were specifically interested in extracting data about the state of the pump's security at the time of the report, who discovered the skimmer, and what data retrieval capabilities the skimmer had. We used generic code "no annotation" if the comment was blank, only mentioned a case number, only mentioned who it was given to, or was solely about some change made after inspection/removal or change in progress. Likewise, we used generic code "unclear" if we did not understand the meaning of the comment in the context of the pump's security. We used code "tape present" if a comment mentioned that tape was present but nothing more about its state. Table IV provides the codebook with frequency counts where both reviewers agreed.

Seal/Tape Conditions. The most common themes among all reports were related to tamper-evident seals. The top two themes among all reports were "tape correctly placed" (929 comments) and "tape incorrectly placed" (79 comments). Other themes for seal and tape conditions were "tape broken" (33 comments), "tape not present" (30 comments), "tape intact" (17 comments), "tape present" (17 comments), "tape was incorrect/fake" (13 comments), and "tape not working" (3 comments). The rate of appearance of seal-related themes highlights the reliance on seals for securing pumps.

The majority of comments mentioned correctly placed seals. One reported skimmer was even found to only have a seal on the pump where the skimmer was located ("This pump had tape intact/all other pumps missing tape/compromised" (821)). While most reports did not note whether the seal was broken, intact, or fake, the provider of the data confirmed that in the majority of cases, the tape is intact and correctly placed. Our analysis could not extrapolate this from the comments, but presence of correctly-placed, intact seals *after skimmer installation* suggests that seals' presence and placement are being attacked.

There are multiple reasons why an intact, correctly placed seal may be present after skimmer installation: the seal may not function correctly (i.e., it removes without indicating tampering), the seal may have been replaced by the adversary (see below), by an employee that did not check for or notice the skimmer, or the skimmer may have been installed from the rear of the unit. Gas pumps are not sealed internally and depending on the model, it is possible to access one side of the terminal through the pump from the other side. In such a scenario, a seal might be broken on the opposite side from where the skimmer is installed ("Pressure Sensitive Security Seal Broken in pump 11. Probably the skimmer in pump 12 was installed through pump 11." (842)). In any of these cases, the seal would not indicate tampering, even if it had occurred. This causes a disconnect between the problem of whether a skimmer is present and whether the seal indicates tampering.

The discovery of fake or incorrect seals also confirms attacks on seal identity. These seals (including branded seals) are available on the Internet, and evaluating whether the identity of the seal is correct requires the consumer or employee to know how the expected seal should look and (if available) the correct serial number. A consumer would likely need to

Code	Count	Example
tape correctly placed	929	All dispensers have correctly placed security tape/unbroken (351)
tape incorrectly placed	79	Improper placement of security tape (389)
no annotation	39	Guardian is currently on site changing the exterior locks and installing the interior security box that encases the card reader board. (358)
discovered by technician	37	Skimmer found by tech while making repairs. (1585)
tape broken	33	All tape was either broken or missing on all pumps (569)
tape not present	30	Did not have security tape but put it on while the Inspector was present (353)
discovered by facility	26	Skimmer found by owner during routine Inspection/Properly placed security tape (446)
high security lock	26	Has high security lock, but no tape. (1269)
Bluetooth skimmer	22	Blue Tooth signal information. Blue Tooth signal: Comfort-Inn High security locks installed on all pumps but not working order during inspection (912)
tape intact	17	All dispensers have correctly placed security tape/unbroken (351)
tape present	17	Pumps have security tape (321)
cellular skimmer	15	All skimmers had cell phone chip. 2 skimmers on pump 1 and 2. on the wire and in the card reader. No security tape. Pump has a high security lock (931)
tape was incorrect/fake	13	Security tape/fake seals were put on/good fake seals (977)
locks not working	10	Blue Tooth signal information. Blue Tooth signal: Comfort-Inn High security locks installed on all pumps but not working order during inspection (912)
education	9	Educated facility staff on identifying skimmers, and ensured they understood proper placement and inspection procedures to ensure the security seals were not tampered with. (1148)
low security lock	9	Locks had not been replaced on Pump #5 & #6 (261)
unclear	8	All nozzles bagged off-out of product/received paperwork on 12/15/16 (313)
extra lock	6	Properly placed security tape/Had extra lock that was ripped open (373)
alarm not working	4	Alarm set for bottom cabinet on dispensers/not top half (cc readers) (345)
discovered by law enforcement	4	No security seals. Pump had standard lock. Skimmer sweep with Hardee County Sheriffs Department. (958)
forced open	4	Properly placed tape and high security lock/pried door open to bend the extra lock (387)
alarm	3	Pumps have properly placed security tape and an alarm (602)
discovered by consumer	3	Consumer complaint for pump 11. I then conducted an inspection of all pumps for skimmers. I found an intact card reader skimmer board on pump 13. This business uses special design Wayne bolts/secondary locks and tapes. The skimmer was removed by tech and given to police (857)
tape not working	3	Inadequate security measures (tape does not show VOID (430)
enhanced security	2	Pumps have properly placed security tape and enhanced security (1069)
high security screws	2	Cell phone chip in skimmer. Enhanced security screws and locks on all pumps (923)
no security measures	2	No security measures All pumps placed out of service (378)
signs of tampering	2	Pumps have properly placed security tape, but there are signs of tampering to the pump (1544)
non-wireless skimmer	1	Pumps have properly placed security tape/1 Bluetooth, 1 thumb drive (529)
vampire clip skimmer	1	Vampire clip found on pump 11 (793)

TABLE IV: Two researchers coded the free-form comments field in the aggregated skimmer report dataset; comments could be coded with multiple labels. This table shows the codebook with examples, sorted by number of occurrences.

inspect multiple seals at the same location to establish whether the seals are consistent and would still be unable to verify the serial number.

Other Measures. Some comments noted the presence and condition of other security measures on pumps at the time skimmers were discovered: "high security lock" (26 comments), "locks not working" (10 comments), "low security lock" (9 comments) "extra lock" (6 comments), "alarm not working" (4 comments), "alarm" (3 comments), "high security screws" (2 comments), and "no security measures" (2 comments).

High security locks were the most commonly mentioned non-seal security measure. These locks are marketed as being difficult to pick and have complex keys that are designed to be more difficult to duplicate.[4] We were interested in how these newer locks are bypassed and our law enforcement contacts described multiple situations in which high security keys were stolen or loaned/bought from a store attendant for hundreds of dollars. In other cases, the locks may be disengaged ("High Security locks & stickers in place/lock wasn't locked" (317)) or broken ("High security locks/broken on pumps 1 & 2" (698)). Accordingly, these locks are insufficient on their own for preventing skimmers and cannot indicate tampering without physical damage.

Skimmer Type. In some cases, the comments specified the capabilities of the skimmer: "Bluetooth skimmer" (22 comments), "cellular skimmer" (15 comments), "non-wireless skimmer" (1 comment), and "vampire clip skimmer" (1 comment).

Vampire clip skimmers attach to the ribbon cable between the card reader and the upstream control circuitry. They clamp over the ribbon cable and break the shielding, allowing the device to tap the connection. These devices require careful placement of the skimmer over the ribbon cable to avoid damaging the connection and are specific to the thickness of the cable being used. We have not yet obtained a vampire clip skimmer, but expect that they have similar retrieval characteristics to other skimmers.

As we discussed in Section IV, the use of Bluetooth, cellular, and non-wireless skimmers prevents commodity consumer hardware from detecting skimmers wirelessly. Skimmers with a variety of data retrieval mechanisms do not present a consistent wireless signature for detection, and this data shows that the types of skimmers we examined earlier are being found in the field.

Discovery. According to our contacts, most skimmers are discovered during routine inspection by the Florida Department of Agriculture and Consumer Services. However, some reports noted who initially found the skimmer: "discovered by technician" (37 comments), "discovered by facility" (26 comments), "discovered by law enforcement" (4 comments), and "discovered by consumer" (3 comments).

Gas pumps are not always managed by the facility's operators, and the business structure of this (leasing, con-

[4]While working with law enforcement, an officer demonstrated to us that some standard pump locks can be opened with an ordinary, unrelated file cabinet key. Don't try this at home.

tracting, etc.) is outside of the scope of this paper. However, we separated phrasing such as "Skimmer found by owner during routing inspection/Properly placed security tape" (446) from "Pumps have properly placed security tape/skimmers found by Pump Tech" (542) into "discovered by facility" and "discovered by technician" respectively in order to capture these distinct groups.

Limitations. To the best of our knowledge, this data is the best available aggregate data for detected skimmers, but it has limitations; all fields are human-generated free responses. Some entries record data about multiple skimmers or multiple pumps at the same facility. The entries also do not specify an exhaustive description of the skimmers or security measures. Since this dataset is long-term, it is possible that how the data was entered or interpreted changed over time.

This data also represents conditions *when skimmers were found*, not when they were installed; the placement of seals and other controls could have occurred after skimmer installation, but this would highlight a similar problem where pumps are not being correctly checked before applying a seal. While this data has been aggregated, the reports come from individual inspectors and other law enforcement officers, so clarification of ambiguous text was not possible. Accordingly, in this section, we have analyzed the data as provided. This data highlights the real-world problems with protecting gas pumps against skimmers.

C. Lessons Learned

In this section, we began by characterizing the only visible security indicator available to consumers for detecting gas pump tampering: tamper-evident seals. Besides being the only visible indicator, these seals are also the least expensive and easiest to deploy by businesses. We defined the properties that whomever evaluates a seal must decide: presence, placement, intent, identity, and indication. We then obtained and analyzed over three years of aggregate data on skimmer detections by the Florida Department of Agriculture and Consumer Services and found that seals are the most frequent security control used on pumps. On pumps *where skimmers have been discovered*, they are most often found with security seals in place. Worse, attacks are reported on 4 of 5 characteristics that must be evaluated on a seal, creating further difficulty for evaluating these seals. Ultimately, these seals do not indicate when a skimmer is present and are easily evaded by adversaries.

VI. Discussion

Based on our analyses of current skimmer detection applications, it is clear that the possible detection methods are limited and can not provide consumers with tools that accurately detect skimming devices. Our analysis of hardware from Section IV is evidence that even with similar constructions, skimmers can vary in methods of data retrieval and no characteristic of this can be guaranteed and used as a method of detection. As long as skimmer detection apps rely on limited methods including Bluetooth scanning, MAC address recognition, and blacklists, the apps will continue to be ineffective and leave the consumer unknowingly vulnerable.

Aside from poorly developed detection tools, we found that tamper-evident seals are also ineffective with helping consumers detect skimming. The seals used at North American gas stations often differ by fuel brand, seal brand, station owner, and placement. We have observed municipal pump seals, branded seals, and generic seals—all in a variety of sizes, colors and fonts. Some have serial numbers; others do not. We have also observed multiple styles of seal on the same pump. Inconsistencies in seal presence, placement, and identity prevent successful consumer evaluation, and our results in Section V demonstrate that resolving these would be a partial solution at best. Our analysis has demonstrated that consumer-facing tools for detecting gas pump skimmers can fall short for a variety of reasons. As skimming technology adapts, the number of available detection mechanisms for consumers dwindles.

A. Countermeasures

Use another required security measure/deprecate seals. As we previously discussed, in Florida, operators are generally required to deploy tamper-evident seals, a device that will disable the terminal when opened, or an encrypting card reader [1]. Our data in Section V shows that tamper-evident seals are overwhelmingly the only control reported present when skimmers are found. Neither disabling devices nor encrypting card readers appeared in reports, suggesting that either these devices are effective or not in use.

Anti-tampering equipment to electronically disable a terminal when opened is common practice among PIN Entry Devices (PEDs) [56]. However, it is unclear if adding these devices to gas pumps is financially feasible or how store operators with a single on-site employee would handle false positives. We discussed in Section V that insider threats are also problematic. If a malicious employee can re-enable the pump, then the disabling device will not be effective. Accordingly, these devices require new processes and handling to work. Encrypting card readers also require additional care in deployment; key management and back-end processing add complexity which may complicate deployment for small businesses.

The correct deployment of either of these technologies effectively renders internal skimmers useless. A disabled pump cannot accept cards and an encrypting reader does not transmit sensitive account data as plaintext. This would make external (i.e., overlay and deep-insert) skimmers the simplest attack at gas pumps; the Skim Reaper system from Scaife et al. is designed to detect these types of attacks [45]. We recommend the removal of tamper-evident seals as a sufficient security measure from existing or future regulation.

Invest in alternative payment mechanisms. Given the prevalence of smartphones (which increasingly offer NFC payment mechanisms), it may be advantageous to merchants to instead invest in wireless payment mechanisms. These technologies typically do not use static account data, reducing the viability of skimming attacks. The apps used for these payments offer fast updates without further hardware updates, which may avoid further costly upgrades. One disadvantage of this approach is that these mechanisms are not inclusive. In order to use wireless payment mechanisms, users need to own a smartphone that has support for such payment methods. Not all people have such a device, and some may not elect to

use such technology even if they did. Gas pumps would still need to continue to support card payment for these individuals resulting in skimmers still being a problem. Another disadvantage to this approach is that malicious terminals are often not considered in attack models for payment systems (and can be exploited in EMV [23]). Given the difficulty operators have securing existing pumps, it may difficult to achieve the needed level of trust with existing technology. Consequently, we believe more work is needed to develop strong controls for wireless pay-at-the-pump technology.

Due to the financial constraints regarding replacing existing terminal hardware (see Section II), we believe this approach is only viable if sufficient consumer demand exists. The initial deployment of pay-at-the-pump technology took approximately two decades to reach ubiquity [36] and was likely driven by consumer demand for a more convenient payment mechanism. Without such demand, terminal replacements seem unlikely without either an authoritative force (e.g., regulation or contractual obligation) or subsidies/discounts to lower the financial burden on businesses. We suspect that force without financial assistance is likely to result in the closure of stores who cannot otherwise afford new technology. We recommend that future research into new types of payment mechanisms consider deployment cost as a feature and that regulators consider how these changes will affect businesses.

Interrupt the payment workflow. Finally, other research from our community [26], [40] suggests that interrupting the payment workflow may be successful in bringing consumers' attention to the security indicators. An on-screen message could display an image of a correct seal, the seal's serial number, and require acknowledgment (e.g., inputting the serial number on the seal) before proceeding. Such a system could conceivably be deployed as a software update to existing hardware, though many existing pumps allow the consumer to begin the transaction by inserting their payment card, which might render a system like this ineffective at preventing skimming. While users might be unwilling to accept an interrupted payment flow, it may be possible to use human interaction to detect tampering similarly to other problems in our community.

This is not a panacea. Even with additional consumer awareness and individually-numbered seals, our analysis shows that attackers actively target these seals. It is likely that attackers would simply adjust their replacement seals to match the on-screen instructions. Accordingly, we do not recommend this mechanism, but we note it here for completeness.

B. Summary

We believe the fastest and most cost-effective solution is to physically enhance the security of gas pumps to deny attackers access to the inside of the unit. Though such security mechanisms for gas pumps are not yet widespread, similar technologies already exist for other payment terminals, and these should be explored before relying on human-based checks for detection.

VII. Related Work

Research in security indicators largely focuses on the interaction between the indicators and the user base [18]. This is most prevalent in web browsers, where visual messaging is critical to informing users of threats to their online safety [22], [47], [57], [27], [8]. Experiments on these indicators show that users notice these far less frequently unless their task is interrupted [26]. Similarly, research has demonstrated that while many webcams use indicators (e.g., lights), they are largely unnoticed until an obvious, red indicator was overlaid onto the user's display [40].

Security indicators are also critical to physical assets including those in healthcare [48], [55], voting machines [29], [14], [55], and payment devices [24]. Tamper-evident seals are intended to convey information about the confidentiality or integrity of an enclosure. Johnston analyzed hundreds of seal designs and found the median time to successfully attack (defeat or spoof) a seal was 43 seconds with a cost of less than one dollar on subsequent attacks [30]. Our research expands this work by exploring these seals when applied to payment systems (specifically, the task of buying fuel).

Payment systems fraud detection research focuses primarily on deciding whether to allow a transaction at the time that transaction occurs [15], [51], [16], [50], [6], [7]. This type of analysis reduces the quantity of magnetic stripe fraud but ignores issues of both illegitimate encoding of correct card data and data acquisition. MagnePrint [2] attempts to resolve the former by measuring a card's magnetic material at manufacture and verifying the measurement upon card use. Since this system requires a priori measurement, it cannot be used to verify previously-issued cards. To address this, Scaife et al. developed a system for using the encoding jitter of the data to distinguish counterfeit writes from originals [46] without needing a measurement during manufacturing. Characterization of skimming attacks has also led to techniques capable of detecting multiple card readers (i.e., overlay and deep-insert skimmers) [45]. These techniques do not apply to other types of skimmers, such as the internal ones predominantly found inside gas pumps. Furthermore, while recent technologies such as EMV payment cards have made duplication more difficult, this has largely moved attacks further into the payment terminal [54], [33], [9], [20], [23], [35], [25], [13], [31], [11]. Understanding detectability of attacks on customer-facing terminals is therefore critical to improving payment systems security.

VIII. Conclusion

Our comprehensive analysis provides strong evidence that consumers have not been given the tools necessary to protect themselves against fraud at the pump. We then showed that while skimmer detection apps are available for the most popular mobile platforms, few can detect any skimmers at all. Moreover, through a forensic analysis of actual skimmers recovered by law enforcement, we demonstrate that those apps that can detect skimmers can trivially be evaded. Finally, through the most comprehensive analysis of skimmers discovered over the course of nearly four years, we show that anti-theft mechanisms such as tamper-evident seals provide little impediment to criminals. Simply arguing that deploying EMV solves the problem ignores the massive expenses and logistical challenges facing the industry; rather, a coordinated effort to protect consumers and reduce fraud must be undertaken.

ACKNOWLEDGMENTS

The authors would like to thank Hal Prince and the Florida Department of Agriculture and Consumer Services, Nick Ferrara of the Gainesville Police Department, Cary Gallop and Joe VanGorder of the Alachua County Sheriff's Office, and the NYPD Financial Crimes Task Force for their invaluable assistance with this work. This work was supported in part by the National Science Foundation under grant number CNS-1526718. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Florida Department of Agriculture and Consumer Services, Gainesville Police Department, Alachua County Sheriff's Office, NYPD Financial Crimes Task Force, or the National Science Foundation.

REFERENCES

[1] "Florida statute section 525.07(10)(a)," https://web.archive.org/web/20181128204140/http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0525/Sections/0525.07.html, 2008.

[2] "Welcome to MagnePrint®: What is MagnePrint?" http://www.magneprint.com/, 2016. [Online]. Available: http://www.magneprint.com/

[3] "Gas pump skimmers," https://web.archive.org/web/20180420143818/https://learn.sparkfun.com/tutorials/gas-pump-skimmers, 2017.

[4] "Skimmer scanner: A gas pump skimmer detection app by sparkx," https://github.com/sparkfunX/Skimmer_Scanner, 2017.

[5] "Welcome to the public listing for ieee standards registration authority," https://regauth.standards.ieee.org/standards-ra-web/pub/view.html, 2018.

[6] A. Agrawal, S. Kumar, and A. Mishra, "Credit card fraud detection: A case study," in *2015 2nd International Confrence on Computing for Sustainable Global Development(INDIACom)*, 2015.

[7] ——, "A novel approach for credit card fraud detection," in *2015 2nd International Confrence on Computing for Sustainable Global Development(INDIACom)*, 2015.

[8] C. Amrutkar, P. Traynor, and P. C. van Oorschot, "Measuring SSL indicators on mobile browsers: Extended life, or end of the road?" ser. Lecture Notes in Computer Science, D. Gollmann and F. C. Freiling, Eds. Springer Berlin Heidelberg, Sep. 2012, pp. 86–103. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-33383-5_6

[9] R. Anderson and S. J. Murdoch, "EMV: Why payment systems fail," *Communications of the ACM*, vol. 57, no. 6, 2014.

[10] Apple, "App store review guidelines," https://developer.apple.com/appstore/resources/approval/guidelines.html, May 2018.

[11] M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, and R. Anderson, "Chip and skim: Cloning EMV cards with the pre-play attack," in *2014 IEEE Symposium on Security and Privacy(S& P)*, 2014.

[12] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa

[13] J. Bukhari, "That chip on your credit card isn't stopping fraud after all," Fortune - http://fortune.com/2017/02/01/credit-card-chips-fraud/, 2017.

[14] K. R. B. Butler, W. Enck, H. Hursti, S. E. McLaughlin, P. Traynor, and P. D. McDaniel, "Systemic issues in the hart InterCivic and premier voting systems: Reflections on project EVEREST," *EVT*, vol. 8, pp. 1–14, 2008. [Online]. Available: https://www.usenix.org/legacy/event/evt08/tech/full_papers/butler/butler.pdf?utm_content=bufferc3cd8&utm_source=buffer&utm_medium=facebook&utm_campaign=Buffer

[15] P. K. Chan, W. Fan, A. L. Prodromidis, and S. J. Stolfo, "Distributed data mining in credit card fraud detection," in *IEEE Intelligent Systems and Their Applications*, 1999.

[16] P. K. Chan and S. J. Stolfo, "Toward scalable learning with non-uniform class and cost distributions: A case study in credit card fraud detection." in *KDD*, 1998.

[17] S. Chandrasekaran, R. Vempati, and D. Dharanalakota, "System and method for detection of rogue routers in a computing network," 2016, uS Patent 9,467,459.

[18] L. F. Cranor, "What do they "indicate?": Evaluating security and privacy indicators," *Interactions*, vol. 13, no. 3, pp. 45–47, May 2006. [Online]. Available: http://doi.acm.org/10.1145/1125864.1125890

[19] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "Imsi-catch me if you can: Imsi-catcher-catchers," in *Proceedings of the 30th annual computer security applications Conference*. ACM, 2014.

[20] J. de Ruiter and E. Poll, "Formal analysis of the EMV protocol suite," in *Theory of Security and Applications*, ser. Lecture Notes in Computer Science, S. Mödersheim and C. Palamidessi, Eds. Springer Berlin Heidelberg, 2011.

[21] E. Delany, "Why Gas Stations Are Late to the Chip Card Game," https://cardconnect.com/company/blog/gas-stations-late-to-chip-card-game, 2017.

[22] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '06. New York, NY, USA: ACM, 2006, pp. 581–590. [Online]. Available: http://doi.acm.org/10.1145/1124772.1124861

[23] S. Drimer and S. J. Murdoch, "Chip & PIN (EMV) relay attacks," https://www.cl.cam.ac.uk/research/security/banking/relay/, 2013.

[24] S. Drimer, S. J. Murdoch, and R. Anderson, "Thinking inside the box: System-Level failures of tamper proofing," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. ieeexplore.ieee.org, May 2008, pp. 281–295. [Online]. Available: http://dx.doi.org/10.1109/SP.2008.16

[25] S. Drimer and S. J. Murdoch, "Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks," in *USENIX Security*, vol. 2007, 2007, pp. 87–102.

[26] S. Egelman, L. F. Cranor, and J. Hong, "You've been warned: An empirical study of the effectiveness of web browser phishing warnings," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '08. New York, NY, USA: ACM, 2008, pp. 1065–1074. [Online]. Available: http://doi.acm.org/10.1145/1357054.1357219

[27] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo, "Rethinking connection security indicators," in *SOUPS*. usenix.org, 2016, pp. 1–14. [Online]. Available: https://www.usenix.org/sites/default/files/soups2016_full_proceedings_interior.pdf#page=7

[28] K. Gunderson, "Protecting your credit card information from skimmers at the gas pump," https://wchstv.com/news/local/protecting-your-credit-card-information-from-skimmers-at-the-gas-pump, May 2017.

[29] J. A. Halderman, E. Rescorla, H. Shacham, and D. Wagner, "You go to elections with the voting system you have: Stop-Gap mitigations for deployed voting systems," *EVT*, vol. 8, pp. 4–4, 2008. [Online]. Available: https://www.usenix.org/event/evt08/tech/full_papers/halderman/halderman_html/

[30] R. G. Johnston, "Tamper-Indicating seals," *American Scientist*, vol. 94, no. 6, pp. 515–523, 2006.

[31] B. Krebs, "Chip card ATM 'shimmer' found in Mexico," https://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/, Aug. 2015, accessed: 2018-1-29.

[32] J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," *Biometrics*, pp. 159–174, 1977.

[33] D. Luca and J. Nocera, "It's time to invest in EMV payment card systems," http://usblogs.pwc.com/cybersecurity/its-time-to-invest-in-emv-payment-card-systems/, 2014.

[34] J. Milliken, V. Selis, and A. Marshall, "Detection and analysis of the chameleon wifi access point virus," in *EURASIP Journal on Information Security*, 2013.

[35] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond, "Chip and PIN is broken," in *2010 IEEE Symposium on Security and Privacy(S& P)*, 2010.

[36] NACS, "The history of gasoline retailing," https://web.archive.org/web/20130114234025/http://www.nacsonline.com:80/NACS/Resources/campaigns/GasPrices_2011/Pages/100PlusYearsGasolineRetailing.aspx, 2011.

[37] NACS, "Some retailers balking at pump upgrade for EMV cards," https://web.archive.org/web/20180507160245/http://www.convenience.org/Media/Daily/Pages/ND1008145.aspx, Oct. 2014.

[38] ——, "Gas stations waiting longer to convert to emv," https://web.archive.org/web/20180507163217/http://www.convenience.org/Media/Daily/Pages/ND0919174.aspx, 2017.

[39] NACS, "Credit and debit card usage at the pump," https://web.archive.org/web/20180506192631/http://www.convenience.org/YourBusiness/FuelsCenter/Pages/Cards-at-the-Pump-A-Primer.aspx, Feb. 2018.

[40] R. S. Portnoff, L. N. Lee, S. Egelman, P. Mishra, D. Leung, and D. Wagner, "Somebody's watching me?: Assessing the effectiveness of webcam indicator lights," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 1649–1658. [Online]. Available: http://doi.acm.org/10.1145/2702123.2702164

[41] O. Post, "Fourth credit card skimmer found," http://www.ocalapost.com/fourth-credit-card-skimmer-found/, Apr. 2015.

[42] L. Project, "Lldb debugger," https://lldb.llvm.org/, 2018.

[43] O. A. V. Ravnås, "Frida: A world-class dynamic instrumentation framework," https://www.frida.re/, May 2018.

[44] H.-R. SA, "Ida pro disassembler," https://www.hex-rays.com/, 2008.

[45] N. Scaife, C. Peeters, and P. Traynor, "Fear the reaper: Characterization and fast detection of card skimmers," in *USENIX Security Symposium*, 2018.

[46] N. Scaife, C. Peeters, C. Velez, H. Zhao, P. Traynor, and D. Arnold, "The cards aren't alright: Detecting counterfeit gift cards using encoding jitter," in *2018 IEEE Symposium on Security and Privacy (S&P)*, 2018.

[47] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The emperor's new security indicators," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*. ieeexplore.ieee.org, 2007, pp. 51–65. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/4223213/

[48] R. Y. Shah, P. N. Prajapati, and Y. K. Agrawal, "Anticounterfeit packaging technologies," *Journal of advanced pharmaceutical technology & research*, vol. 1, no. 4, pp. 368–373, Oct. 2010. [Online]. Available: http://dx.doi.org/10.4103/0110-5558.76434

[49] P. Software, "Jeb decompiler," https://www.pnfsoftware.com/jeb/, 2018.

[50] A. Srivastava, A. Kundu, S. Sural, and A. Majumdar, "Credit card fraud detection using hidden markov model," in *IEEE Trans. Dependable Security Comput.*, 2008.

[51] S. Stolfo, D. W. Fan, W. Lee, A. Prodromidis, and P. Chan, "Credit card fraud detection using meta-learning: Issues and initial results," in *AAAI-97 Workshop on Fraud Detection and Risk Management*, 1997.

[52] C. Tressler, "Avoid skimmers at the pump," https://web.archive.org/web/20180720143951/https://www.consumer.ftc.gov/blog/2017/06/avoid-skimmers-pump, Jun. 2017.

[53] ——, "Best practices to foil gas station skimmers," https://web.archive.org/web/20180720143902/https://www.ftc.gov/news-events/blogs/business-blog/2017/06/best-practices-foil-gas-station-skimmers, Jun. 2017.

[54] C. Uriarte, "Gift Card Fraud Will Be a Major Threat Post-EMV," https://www.paymentssource.com/opinion/gift-card-fraud-will-be-a-major-threat-post-emv, 2015.

[55] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp, "Security analysis of india's electronic voting machines," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, ser. CCS '10. New York, NY, USA: ACM, 2010, pp. 1–14. [Online]. Available: http://doi.acm.org/10.1145/1866307.1866309

[56] J. Woolley, "Anti-tampering mechanisms on Ingenico PED," https://www.youtube.com/watch?v=2N06SUHx56k, Mar. 2017.

[57] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '06. New York, NY, USA: ACM, 2006, pp. 601–610. [Online]. Available: http://doi.acm.org/10.1145/1124772.1124863